SONY

“Classic” Technology Presentation

for DSTAC

Brant Candelore
Sr. Staff Member / Passage Architect / Security Specialist
UX Technology Center – San Diego
Sony Electronics Inc.

March 17, 2015

Passage Technology

- Passage Technology
  - Overview (4 slides)
  - Selective Multiple Encryption and Packet Swapping
- Background
  - “Critical Packets” Criteria
  - Licensing and status
  - Security
    - Reports, countermeasures
- Field Implementations

SONY

passage

Overview (4 Slides)

What is Passage?

- Enables flexible, cost-effective CA or DRM interoperability
- Allows service operators to have choice
  - Applications, equipment and devices built around alternate CA or DRM
- Uses Selective Multiple Encryption and Packet Swapping

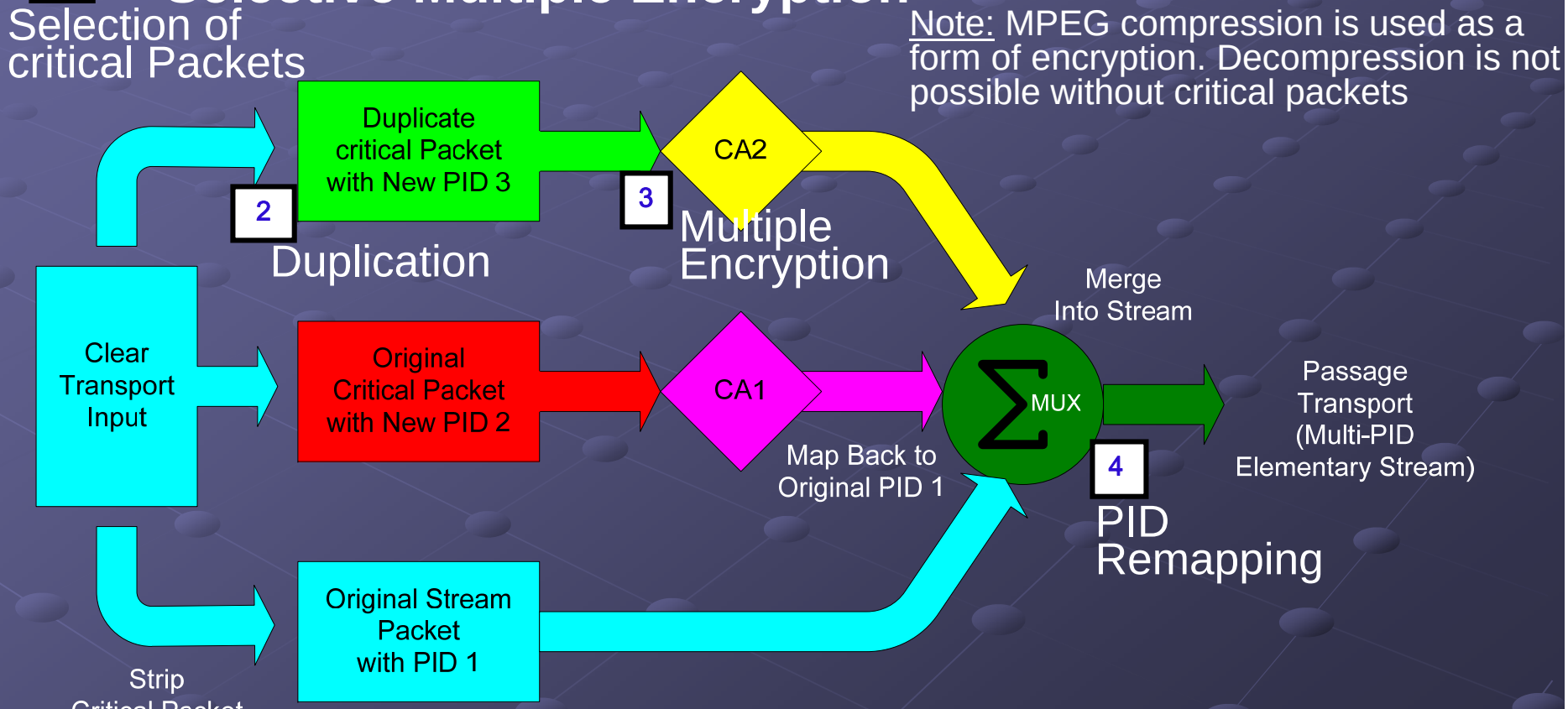
Selective Multiple Encryption: A small amount of critical data, essential for decompressing content is duplicated and encrypted at least two ways

Packet Swapping: Each device receives the same stream, selects its respective encrypted data and shares the remaining common content sent in the clear. “Packet swapping” is used to exchange the legacy CA packet for the alternately encrypted CA or DRM packet

Passage Headend Encoding

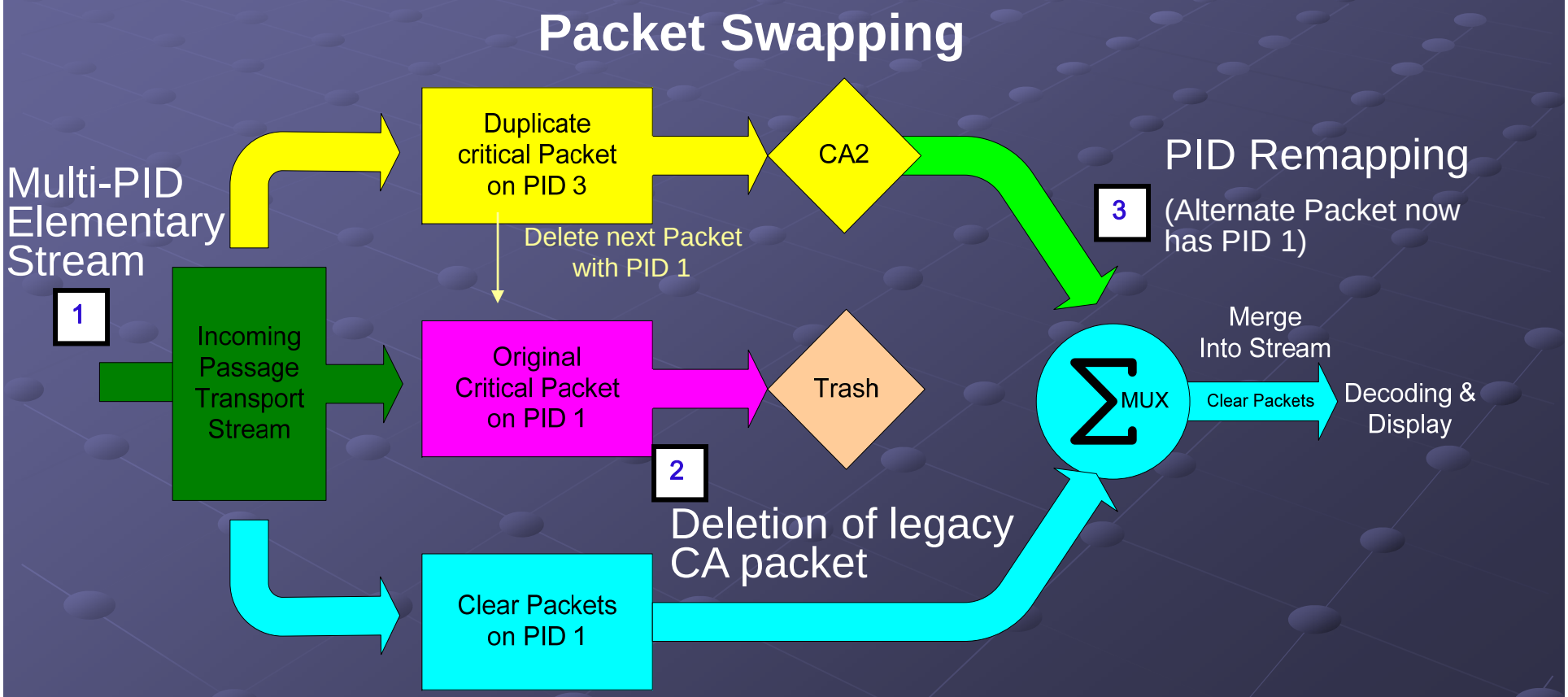
- A the headend, Passage uses 4 basic techniques:
  - Selection of critical packets (headers, etc.)
  - Duplication of selected packets
  - Multiple encryption of duplicated packets
  - Packet Identifier (PID) remapping

1 Selective Multiple Encryption



Passage Device Decoding

- In the device, Passage uses 3 basic techniques:
  - Receipt of structured, multi-PID elementary stream
  - Deletion of legacy PID packet after receipt of alternate PID packet
  - Decryption before Remapping of packet



Passage Summary

- Merits
  - CA agnostic
  - No dependency on legacy CA vendor or licensing
  - Legacy devices are completely unaffected
  - Secure, proven technology with equipment, set-top box & chip support
  - Requires minimal changes (existing mux, stream groomer may be used)
  - Enables flexibility in equipment and mobile devices, TVs, etc.
- Overhead
  - Requires small amount of additional bandwidth (.2 - 1%)
  - Enabling a device for Passage requires minor modification
  - Broadcast plant may require additional control computer equipment

SONY

Expanded Discussion

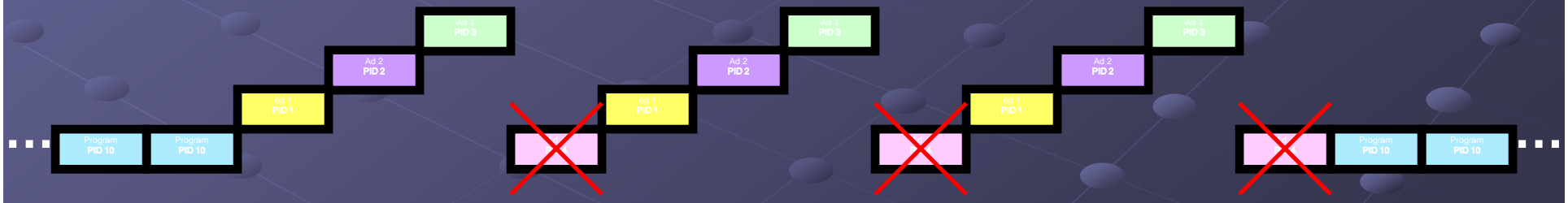
"Packet Swapping" Modes:

Substitution and Insertion

Substitution Mode

- One-for-one substitution, allows for legacy (default) operation
- Decoder Behavior
  - Tune primary and secondary PID
  - Current SOC behavior: When a secondary packet is received, insert it into stream and delete the next primary packet. Deletion effect is a single primary packet.
  - Used by Conditional Access (CA) Overlay application

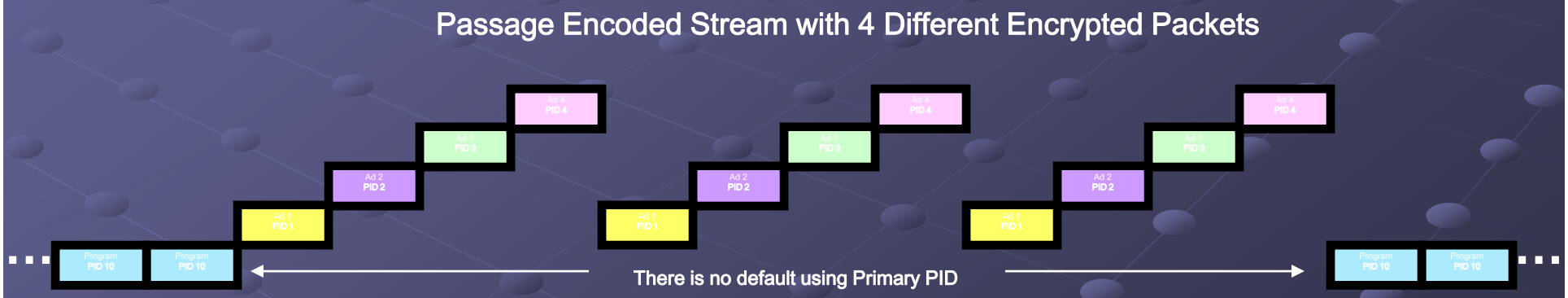
Passage Encoded Stream with 4 Different Encrypted Packets



Main Mode for CA Overlay

Insertion Mode

- Simplest Mode, but does not allow a legacy (default) operation
- Decoder Behavior
  - Tune primary and secondary PID
  - When secondary packet is received, insert it into stream decoded
  - When primary packet is received, insert it into stream as normal
  - No special ordering of packets



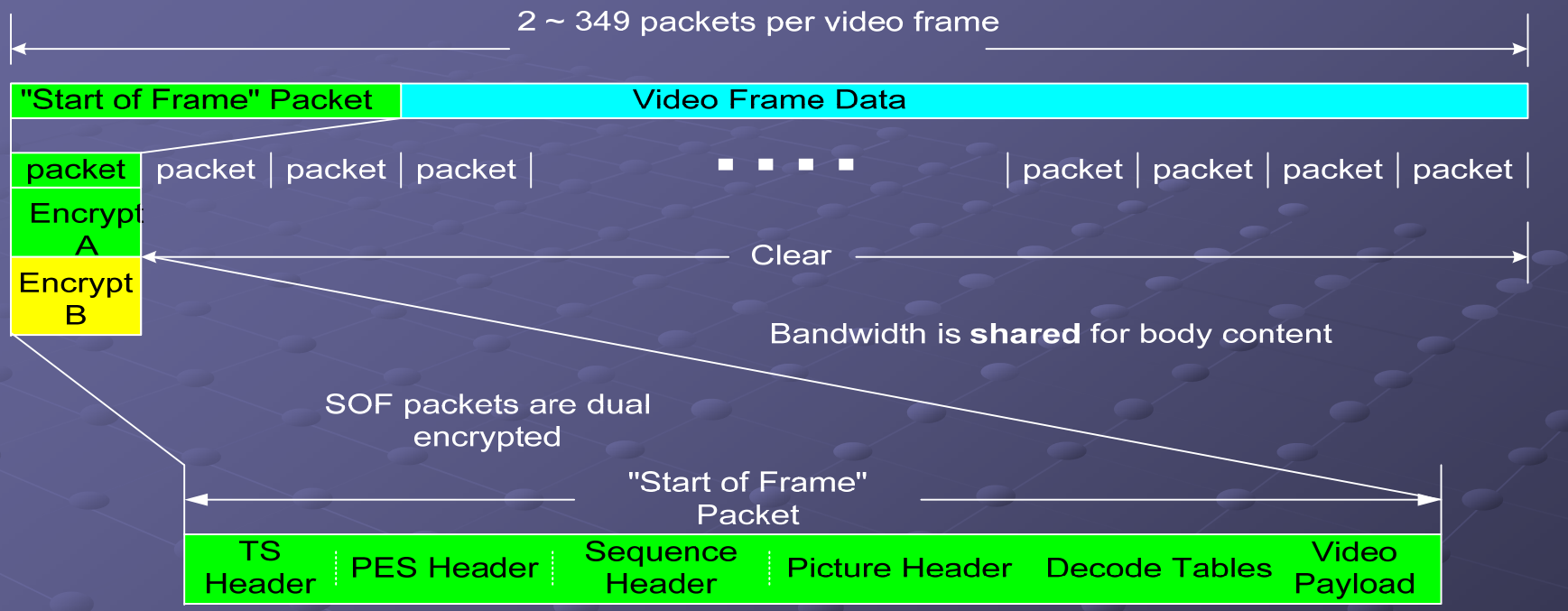
SONY

Critical Packets

Critical Data – Headers

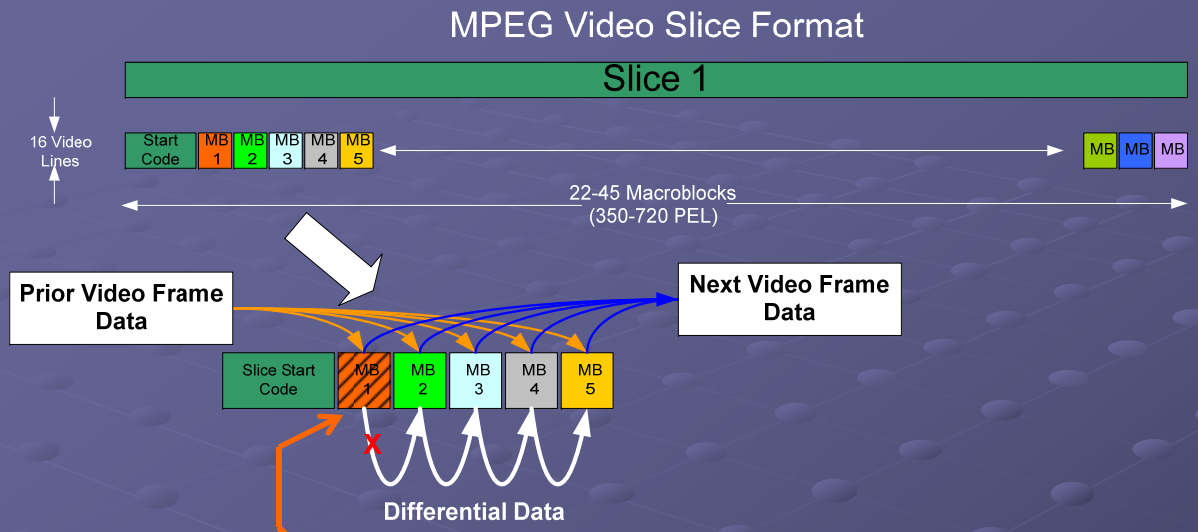
Sequence	Picture Size Frame Rate, Bit Rate Buffering Requirements Programmable Coding Parameters
GOP	Random Access Unit SMPTE Time-Code
Picture	Timing information (buffer fullness, temporal ref) Coding type (I, P, or B)
Slice	Intra-frame addressing information Coding re-initialization (error resilience)

Frame Header Critical Data



Example I-Frame Header

Slice Header Critical Data



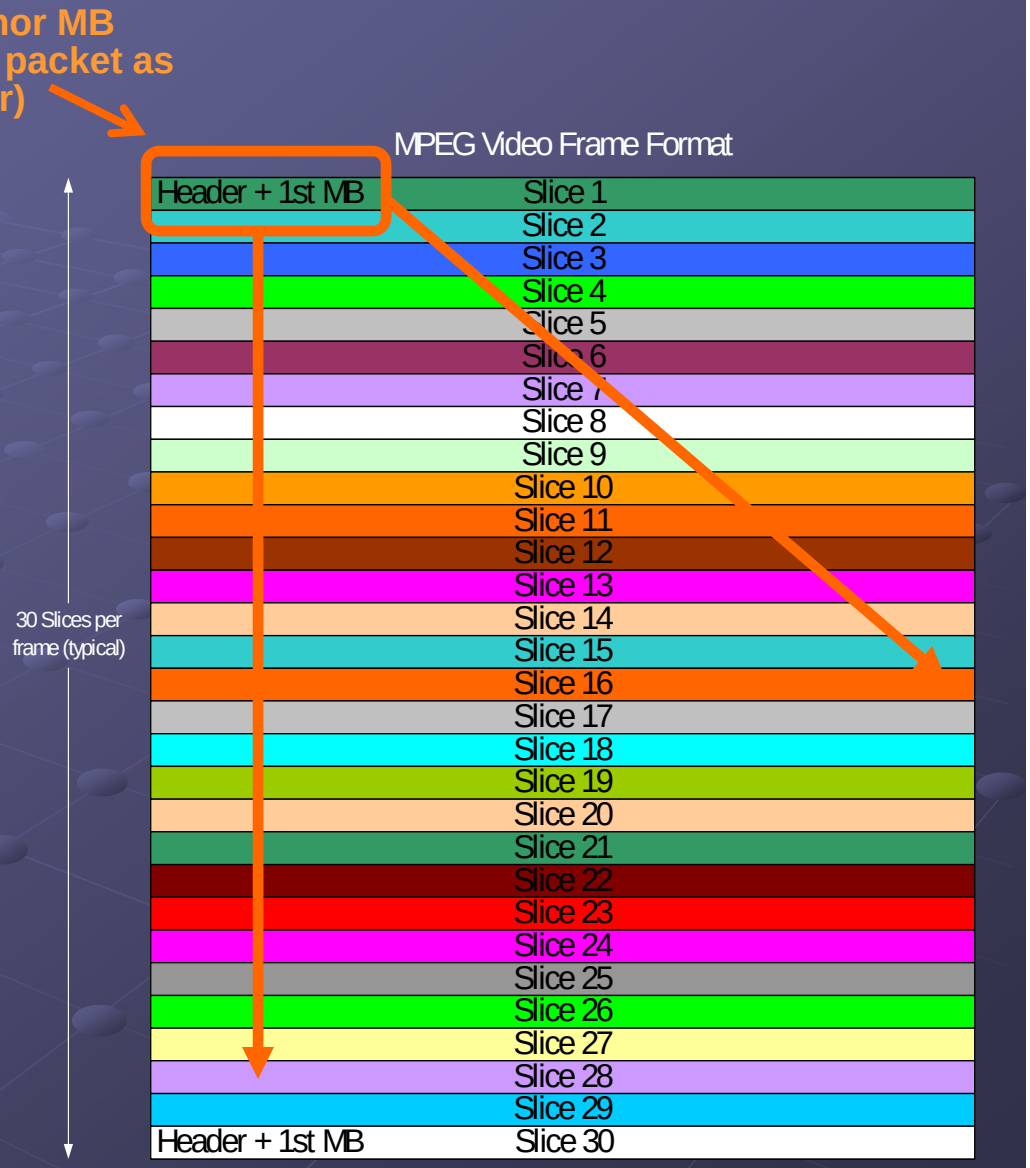
Intercoded Slices: Luminance and Chrominance anchor data

Intracoded Slices: Motion vector anchor data

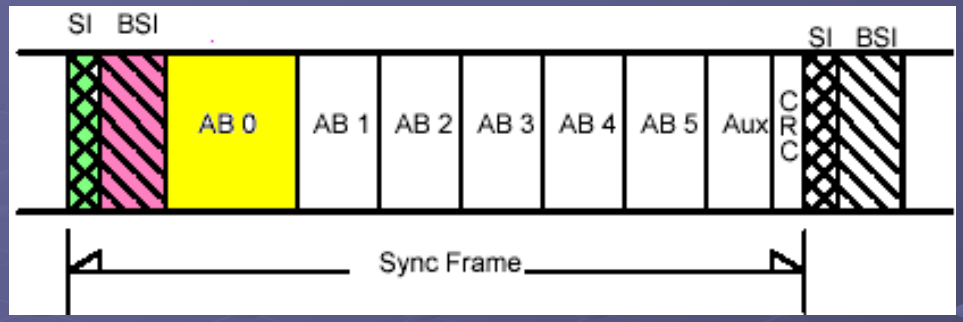
- Each video frame is organized as a series of slices, typically 30 per frame for SD video formats
- Each SD slice is made up of 22 to 45 macroblocks
- Macroblocks in P & B frames are differentially coded to both the previous block and previous video frame
- Removal of the start code & 1st macroblock disrupts the remainder of the slice & other pictures referencing the slice

AVC Critical Data

- AVC uses same transport as MPEG2 and shares the same constructs: frames, slices, and macroblocks (MBs)
- AVC uses more compression and so excluding header or master macroblock information causes even more problems for reverse engineering
- In MPEG2, slices are independent. The header of each slice is critical
- With AVC, slices can be differentially encoded to the previous slice and the first MB



AC-3 Audio Critical Data



- AC-3 has a simpler hierarchy than MPEG compression and fewer points for synchronization
- Audio Block 0 (AB 0) contains absolute exponent info, referenced by Audio Blocks 1–5, and actual audio data
- Audio typically represents about 5% of total transport bandwidth
- ***Passage*** research reduced into the encoding of AB 0 reduced overhead to .4% of total transport bandwidth

SONY

passage

Bandwidth Overhead
vs.
Modes

Passage Overhead (Video)

PASSAGE VIDEO PACKET AND % BANDWIDTH CALCULATION

Assumptions:	Frms/s	30	GOP	15	Mb/s:	MPEG2	SD 2.5	HD 9.4	AVC	SD 1.5	HD 6

		MPEG2						AVC					
#	Passage Mode Description	Packets/ Frame SD	# of Packets/ second SD	% BW SD	Packets/ Frame HD	# of Packets/ second HD	% BW HD	Packets/ Frame SD	# of Packets/ second SD	% BW SD	Packets/ Frame HD	# of Packets/ second HD	% BW HD
1	**Just I-Frame Headers** (Decoder will not start)												
	I-Frame Headers **Total:**		2	0.12%		2	0.03%		2	0.20%		2	0.05%
2	**I & B Frame Headers**												
	I-Frame Headers	1	2	0.12%	1	2	0.03%	1	2	0.20%	1	2	0.05%
	P-Frame Headers	1	8	0.48%	1	8	0.13%	1	8	0.80%	1	8	0.20%
	B-Frame Headers	1	0	0.00%	0	0	0.00%	1	0	0.00%	1	0	0.00%
	Total:		10	0.60%		10	0.16%		10	1.00%		10	0.25%
3	**All Frame Headers**												
	I-Frame Headers	1	2	0.12%	1	2	0.03%	1	2	0.20%	1	2	0.05%
	P-Frame Headers	1	8	0.48%	1	8	0.13%	1	8	0.80%	1	8	0.20%
	B-Frame Headers	1	20	1.20%	0	20	0.32%	1	20	2.01%	1	20	0.50%
	Total:		30	1.80%		30	0.48%		30	3.01%		30	0.75%
4	**Alternate Slices** (Lower/upper slices are not protected)												
	I-Frame Headers	1	2	0.12%	1	2	0.03%	1	2	0.20%	1	2	0.05%
	I-Frame Slice Headers	13	26	1.56%	25	50	0.80%	5	10	1.00%	5	10	0.25%
	P-Frame Slice Headers	8	64	3.85%	10	80	1.28%	2	16	1.60%	2	16	0.40%
	Total:		92	5.53%		132	2.11%		28	2.81%		28	0.70%

Mode 1 (I-Frame Headers)

FRAME #		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
FRAME TYPE		I	B	B	P	B	B	P	B	B	P	B	B	P	B	B	I	B	B	P	B	B	P	B	B	P	B	B	P	B	B
	Header																														
SLICES	1																														
	2																														
	3																														
	4																														
	5																														
	6																														
	7																														
	8																														
	9																														
	10																														
	11																														
	12																														
	13																														
	14																														
	15																														
	16																														
	17																														
	18																														
	19																														
	20																														
	21																														
	22																														
	23																														
	24																														
	25																														
	26																														
	27																														
	28																														
	29																														
	30																														

Picture Header Encrypted Slice Header Encrypted Slice Content Encrypted Unencrypted

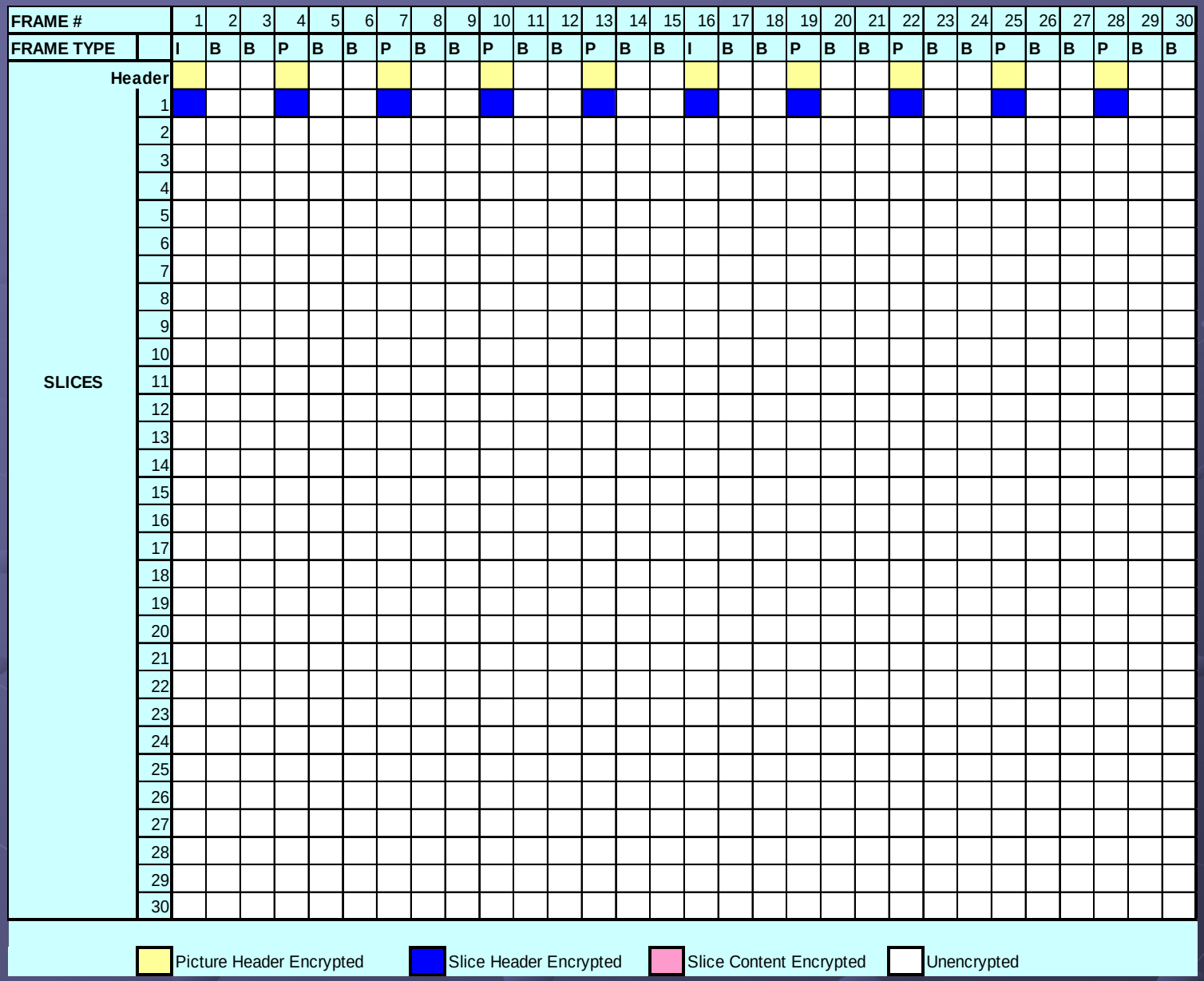
Encrypted Packets

2 packet/s

Standard Definition AVC

0.2%

Mode 2 (I and P-Frame Headers)



Encrypted Packets

10 packet/s

Standard Definition AVC

1.0%

Mode 3 (I,B and P-Frame Headers)

FRAME #		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
FRAME TYPE		I	B	B	P	B	B	P	B	B	P	B	B	P	B	B	I	B	B	P	B	B	P	B	B	P	B	B	P	B	B
	Header																														
SLICES	1																														
	2																														
	3																														
	4																														
	5																														
	6																														
	7																														
	8																														
	9																														
	10																														
	11																														
	12																														
	13																														
	14																														
	15																														
	16																														
	17																														
	18																														
	19																														
	20																														
	21																														
	22																														
	23																														
	24																														
	25																														
	26																														
	27																														
	28																														
	29																														
	30																														

Picture Header Encrypted Slice Header Encrypted Slice Content Encrypted Unencrypted

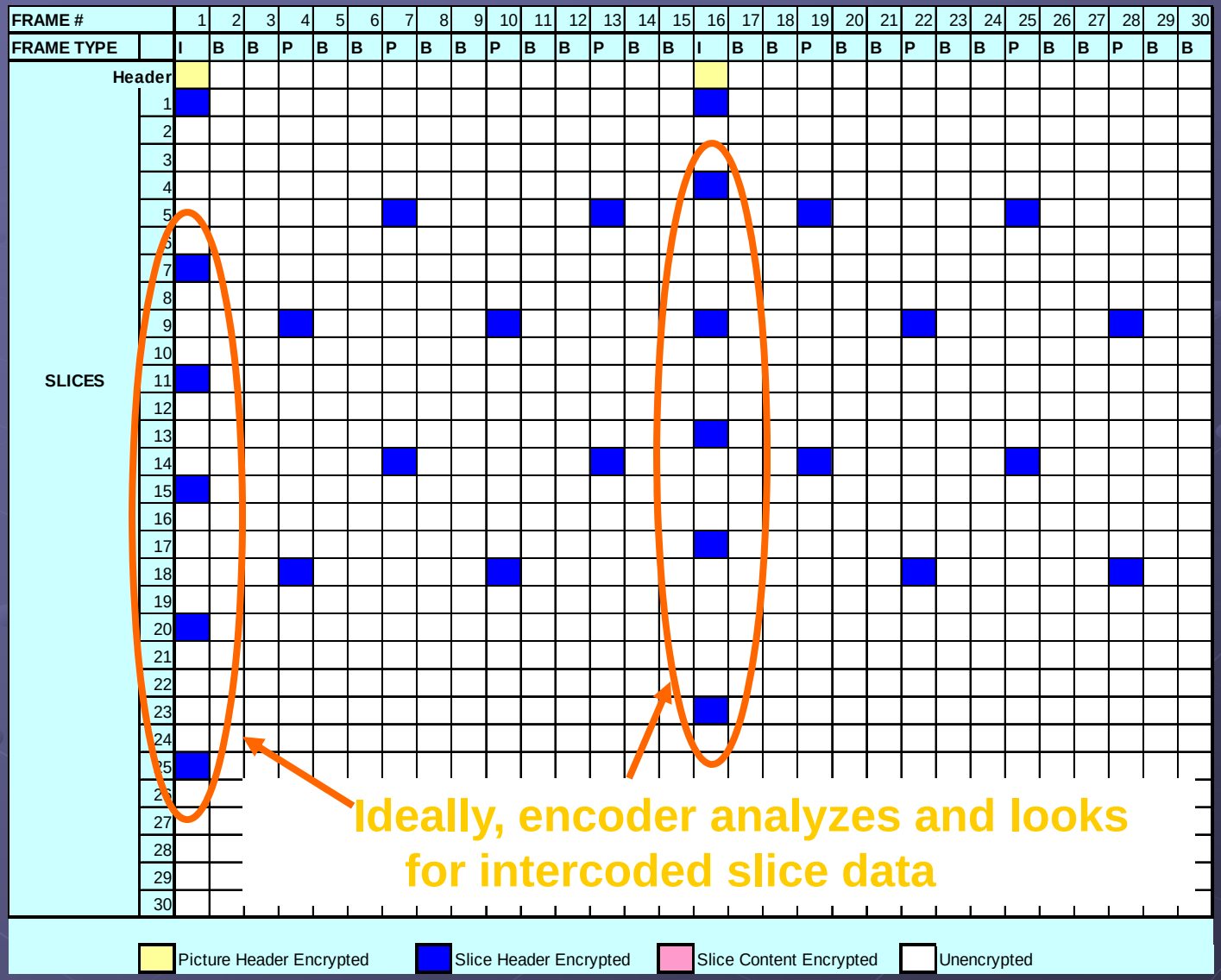
Encrypted Packets

30 packet/s

Standard Definition AVC

3.0%

Mode 4 (I-Frame and Slice Headers)



Encrypted Packets

28 packet/s

Standard Definition AVC

2.8%

SONY

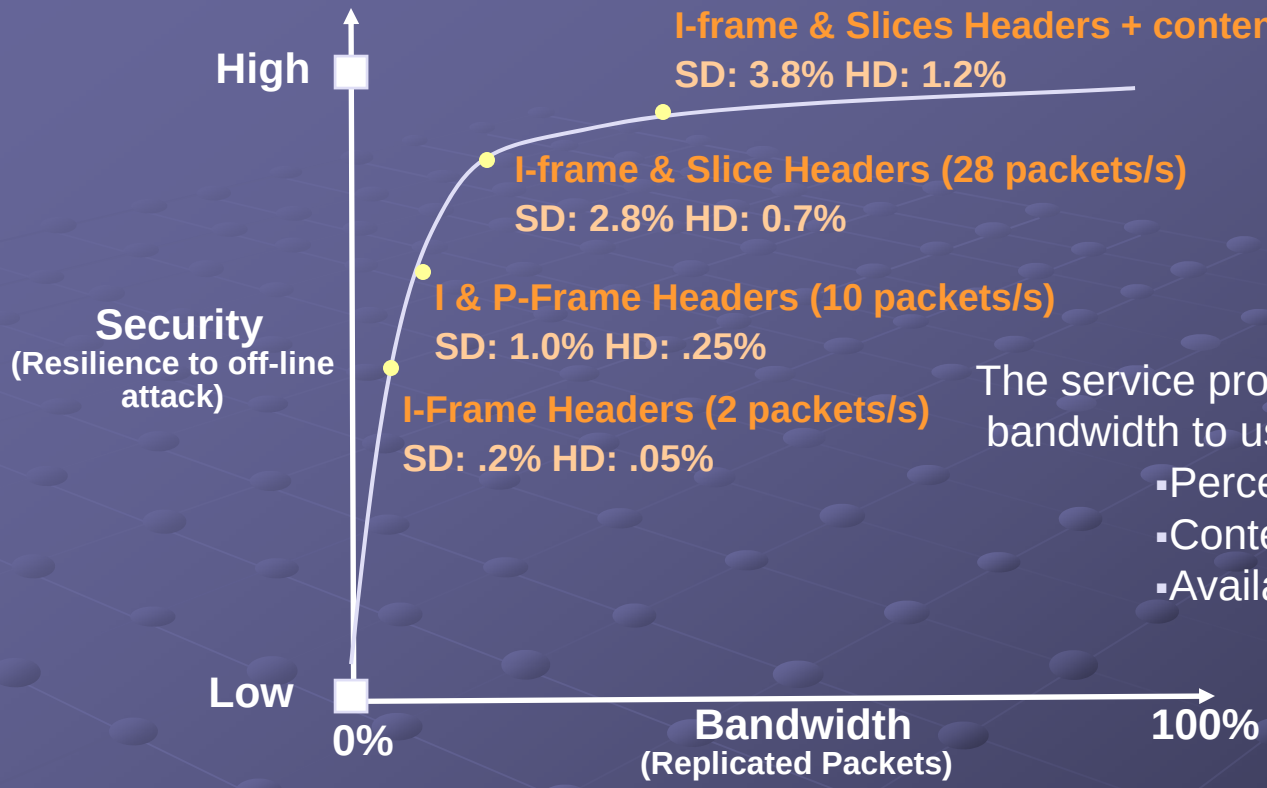
Security Evaluation

Passage Security
Third-Party Security Analysis

Analysts – Sarnoff Laboratories and Merdan Associates:

- Both Sarnoff and Merdan agree that ***Passage*** will cause commercially available decoders to display a blank screen with no audio
- Both Sarnoff and Merdan agree that ***Passage*** encoding of the audio is completely unrecoverable using a modified decoder
- Sarnoff believes that slice header encryption will significantly degrade the image quality of even a modified decoder to make it unwatchable
- Merdan believes that some degraded image fragments may be "watchable", depending on picture content & scene complexity
  - Video image quality is very subjective, and "acceptable video quality" is open to wide interpretation
- Sony believes that the overall video quality is so greatly impacted and with no audio as to render any fragments completely unwatchable

Passage Bandwidth Usage



The service provider chooses the ***Passage*** bandwidth to use based upon:

- Perceived value of content
- Content provider requirements
- Available transport bandwidth

- No significant increase in robustness against offline (PVR) theft is gained when the total ***Passage*** replicated packet BW exceeds 5% SD 2% HD AVC
- Even the lowest level of ***Passage*** application provides complete coverage from real-time, casual theft of service from STBs

SONY

passage

Navigation Information Delivery

Program Specific Information Auxiliary PSI for Passage

- Auxiliary Program Association Table (PAT) is sent on a configurable, network dedicated PID instead of PID 0
- Auxiliary PAT points to auxiliary Program Map Tables (PMTs) that define both primary and secondary (shadow) PIDs for each program
  - Passage enabled STBs tune the auxiliary PSI structure exclusively
  - An additional descriptor in the shadow PMT provides the location of the shadow packets
- Legacy STBs never know about the auxiliary PAT and auxiliary PMTs. They continue to receive the original, unmodified PSI
  - The incumbents cannot claim their PSI or CA structure has been altered
  - The parallel PSI structure is less invasive and assures compatibility with legacy STBs and their proprietary CA systems

Industry Press Reactions

- ***February 9 2004, MultiChannel News wrote:***
  - *"The Sony technology is terrific for transition scenarios"*
  - *"Comcast Corp gave Sony Corp's Passage technology a key stamp of approval"*
- **April 2003, *Cable and Satellite International Magazine* wrote:**
  - *"Opening up the cable industry infrastructure will most certainly foster competition and result in more choices and better services for consumers."*
- **September 2003, *Forbes* wrote:**
  - *"Comcast's Fellows hopes Passage will push box prices down to $50, freeing up capital to speed the digital cable rollout."*
- **March 24, 2003, E-media Magazine wrote:**
  - *"Some are calling this the "Holy Grail" of the cable world-a pretty strong characterization, but one that may well be true."*
- **Feb. 1, 2003, *CED Magazine* wrote:**
  - *"Sony has figured out that the only way to establish a competitive retail market for set-top boxes is to break down control over the CA system and the OOB channel. The Sony theory is elegant."*
- **Dec. 2002, *CED Magazine* wrote:**
  - *"Sony Corp.'s "Passage" technology … could make the set-top sector a very interesting (and more competitive) place"*

SONY

passage

Example
Local Headend Integration

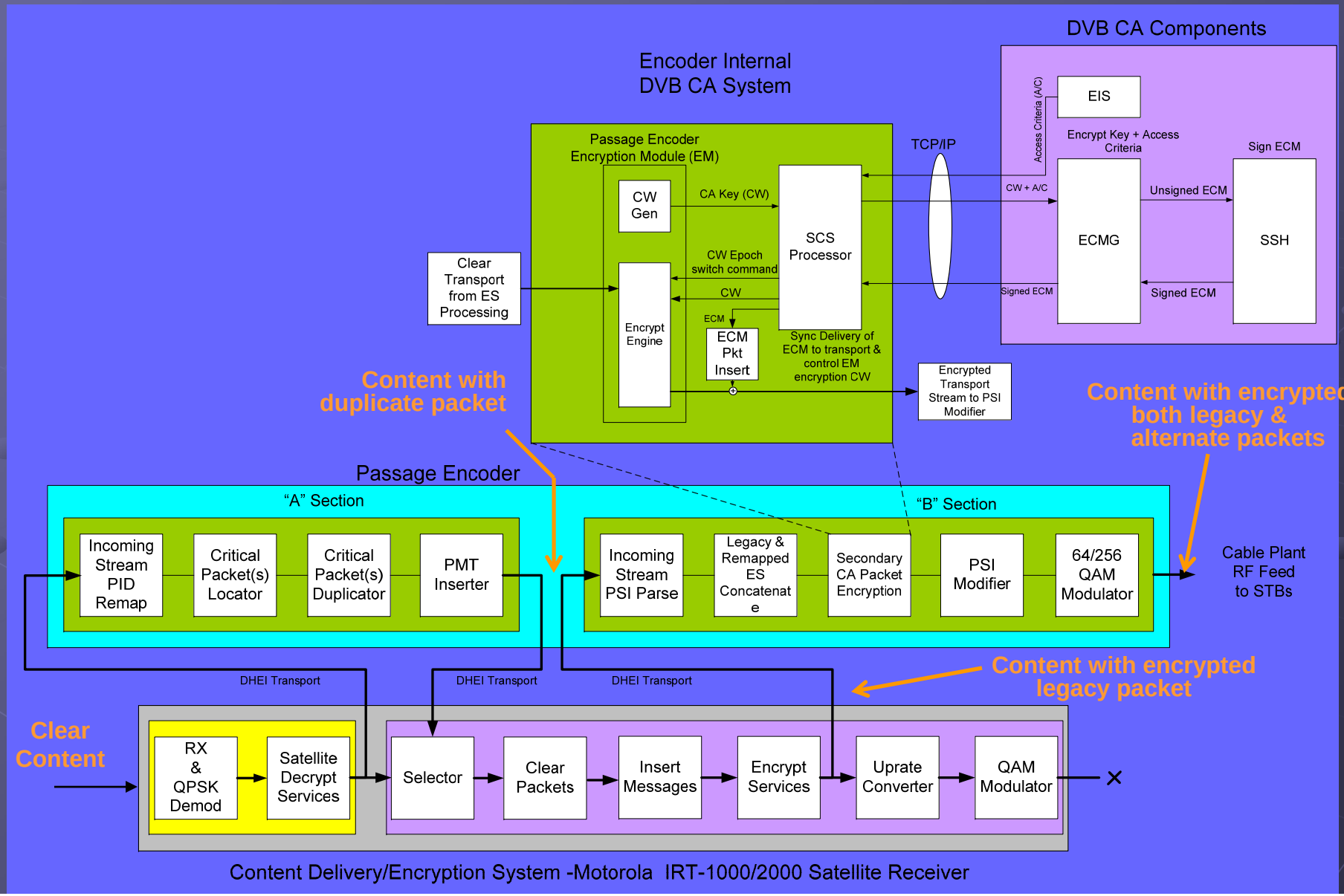
Passage Enabled Headend Field and Lab Trials

- 10 HITS transports
  - 101 Digital channels
  - 45 Music Choice services
- DOCSIS to Passage STBs
- OOB to legacy STBs
- Sony EPG server & 14 day guide
- Legacy and Alternate CAS
- Minimized footprint (24 Sq. Feet)
- System & network monitoring

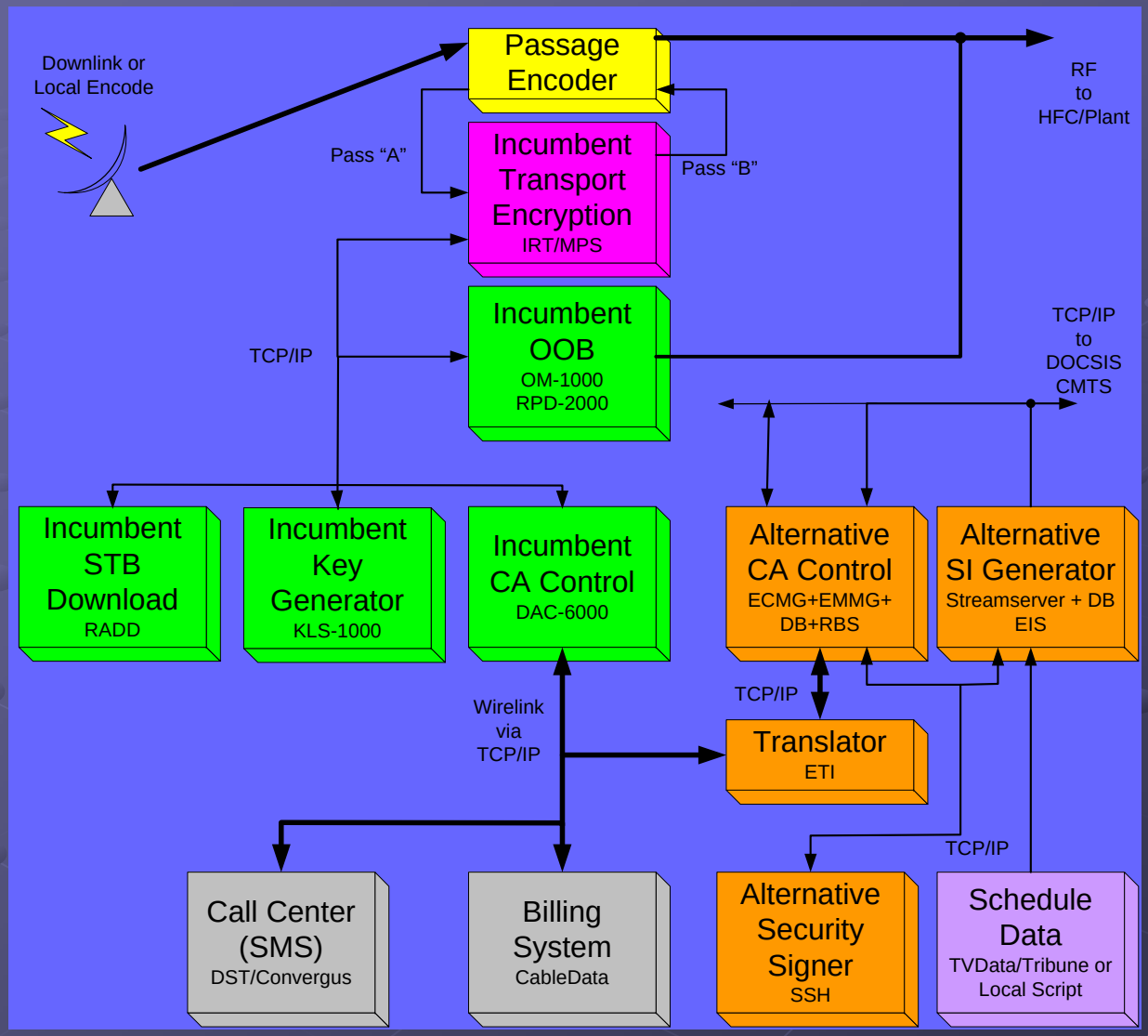
Field Trials: 2 Major MSOs (“public” announcements)

Lab Trials: “1 Major MSO”, “STB vendor” (private investigations)

Passage Integration



Integration



SONY

Thank You!